# *Integrating Information Assurance into NSA Acquisition Programs*

**Briefing to NSA**
**21 September 2005**
**Linthicum, MD**

**Art King (IBM)**
**Dominic Cussatt (IBM)**
**Acquisition Team, DIAP**
**703.604-1480 x-104**
**Arthur.king.ctr@osd.mil**

# Session Objectives

- Present current policy, guidance, and information concerning the implementation of IA into the acquisition process **and** into the systems being acquired.
- Review the typical chronology for implementing IA throughout the acquisition life cycle – The IA Roadmap
- Present an overview of the Acquisition IA Strategy document, including:
  - Determining if an Acquisition IA Strategy is required
  - Key elements of the strategy
  - Preparation, review and approval process
  - Synchronization with other acquisition documents
- Identify additional resources for information

# Session Agenda

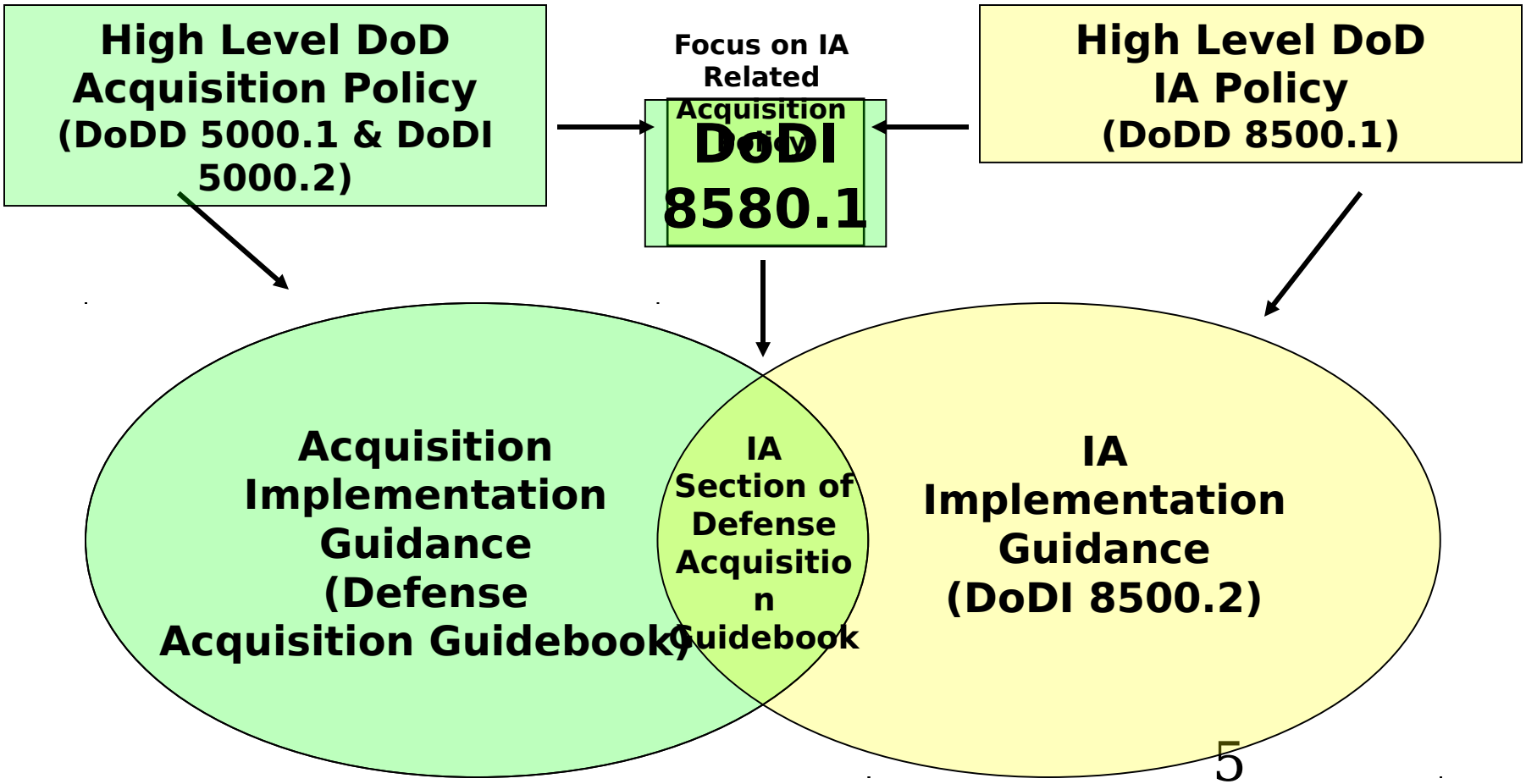
- **The Big Picture** A high level look at IA in acquisition, including:
  - Governing policy and guidance
  - Determining the IA compliance requirement [Does this program need IA? How much?]
- **The IA Roadmap** A summary of the cradle-to grave activities for the notional acquisition program. This portion of the presentation will be keyed to the normal chronology of the acquisition process.
- **The IA Strategy Document** An overview of the OSD template.
- **Resources** Where to go for information and support.
- **Q&A**

# The Big Picture

- Policy and Guidance
  - DoDI 5000.2 “Operation of the Defense Acquisition System”
  - DoDD 8500.1 “Information Assurance”
  - DoDI 8500.2 “Implementing Information Assurance”
  - DoDI 8580.1 “Information Assurance in the Defense Acquisition System”
  - Defense Acquisition Guidebook

# Policy and Guidance

"Where it fits"


High Level DoD Acquisition Policy (DoDD 5000.1 & DoDI 5000.2)
Focus on IA Related Acquisition
DoDI 8580.1
High Level DoD IA Policy (DoDD 8500.1)
Acquisition Implementation Guidance (Defense Acquisition Guidebook)
IA Section of Defense Acquisition Guidebook
IA Implementation Guidance (DoDI 8500.2)

# *"Does this program need to comply with DoD 8500 series?"*

| Acquisition Programs for: | | Acquisition IA Strategy | Compliance with 8500 series |
|---|---|---|---|
| No IT | | Not Required | Not Required |
| Non-MC/ME AIS | | Not Required * | Required |
| Non-MC/ME MAIS | | Not Required * | Required |
| MC/ME AIS | | Required | Required |
| MC/ME MAIS | | Required | Required |
| Outsourced IT-based Processes | | Not Required * | Required |
| Outsourced IT-based Processes that are MC/ME | | Required | Required |
| Platform IT products/weapons systems that are, or have: | | | |
| MC/ME | Network Interconnections to the GIG | | |
| No | No | Not Required * | *Recommended* ** |
| No | Yes | Not Required * | Required |
| Yes | No | Required | *Recommended* ** |
| Yes | Yes | Required | Required |

Legend:
AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical/Mission Essential
PM = Program/Project Manager

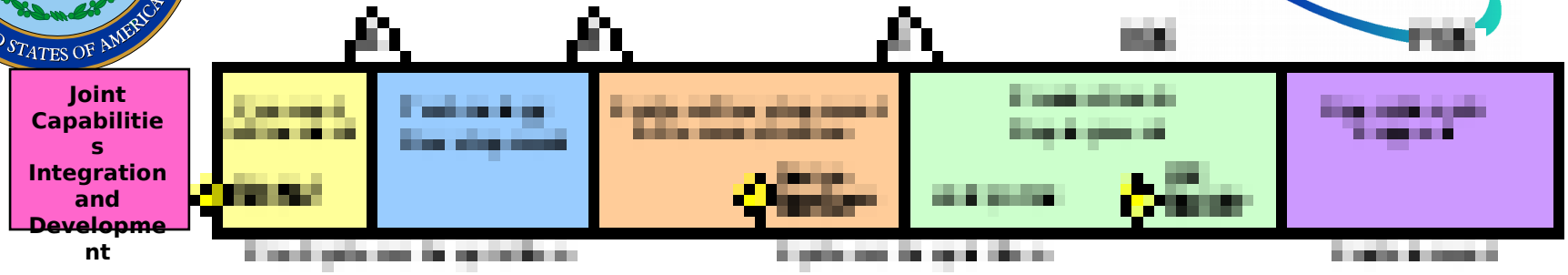
* Although not required by DoD, the Component may require an Acquisition IA Strategy.
** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system

Source: Defense Acquisition Guidebook, Table 7.5.5.1. " IA Compliance by Acquisition Program Type"

# The IA Roadmap

- DoDI 8580.1: "IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire life cycle of the acquisition."
- The IA Roadmap provides a mapping of IA activities to the familiar Defense Acquisition Management Framework.

# Information Assurance Roadmap




1. Specify IA capabilities
2. Establish an IA organization
3. Identify IA requirement
Develop acquisition IA strate
Update
Update
Update
5. Secure resources for IA
6. Conduct C&A process
7. Implement IA solutions
8. Test and evaluate IA solutions
OA Fielded Systems
9. Accredit the system
10. Maintain system security posture throughout life-cycle

# IA Roadmap
## Capsule Step Descriptions

1. Specify required IA Capabilities
   - Initial Capabilities Document (ICD)
   - Mission Assurance Category/Confidentiality Level
   - Net-Ready KPP – IA component
   - Specific IA KPP or performance requirement
2. Establish an IA organization
   - Trained IA professional as IA Manager
   - IA support – organic/matrixed/contracted
3. Identify IA requirements
   - Specified in Requirements/Capabilities Documents
   - Baseline IA Controls
   - Other requirements (e.g. IPv6, DoD PKI)
   - Security Requirements Traceability Matrix

# IA Roadmap
## Capsule Step Descriptions

4. Develop an acquisition IA strategy
   - Required for Mission Critical/Mission Essential IT systems; recommended for others
   - Approved by Component CIO
   - ACAT 1AC, ACAT 1AM and ACAT 1D reviewed by DoD CIO
5. Secure resources for IA
   - Include IA in program budget
   - Determine funding sources
6. Conduct C&A Process
   - Begin Phase I SSAA effort
   - Phase I SSAA should be signed at/near MS-B

# IA Roadmap
## Capsule Step Descriptions

### 7. Implement IA solutions

- Systems Security Engineering efforts
- Procurement of IA/IA enabled products
- Implementing security policies, plans, procedures
- IA Training
- Some may be provided from enclave, infrastructure, or enterprise

### 8. Test and evaluate IA solutions

- Developmental Test (DT)
- Security Test & Evaluation, C&A activities
- Operational Test (OT )

# IA Roadmap
## Capsule Step Descriptions

9. Accredit the system
   - C&A Phase III completed
   - ATO/IATO should be issued prior to MS-C

10. Maintain the system's security posture throughout its life-cycle
   - Periodic assessments
   - Re-accreditation minimum of 3 years
   - "Fielded System" assessments by Operational Test Authority (OTA)
   - Vulnerability reporting and remediation

# Acquisition IA Strategy Document

- Requirement in DoDI 5000.2 and DoDI 8580.1
- Content driven by current lifecycle phase
- High-level perspective
  - Supporting detail not desired in the document
  - Not graded by weight
  - Most programs < 12 pages
- Recommend WIPT involvement to gain stakeholder buy-in
- We will provide **informal** “early coordination” at any time (earlier is better)

# "Does this program need an Acquisition IA Strategy?"

| Acquisition Programs for: | | Acquisition IA Strategy | Compliance with 8500 series |
|---|---|---|---|
| No IT | | Not Required | Not Required |
| Non-MC/ME AIS | | Not Required * | Required |
| Non-MC/ME MAIS | | Not Required * | Required |
| MC/ME AIS | | Required | Required |
| MC/ME MAIS | | Required | Required |
| Outsourced IT-based Processes | | Not Required * | Required |
| Outsourced IT-based Processes that are MC/ME | | Required | Required |
| Platform IT products/weapons systems that are, or have: | | | |
| MC/ME | Network Interconnections to the GIG | | |
| No | No | Not Required * | *Recommended* ** |
| No | Yes | Not Required * | Required |
| Yes | No | Required | *Recommended* ** |
| Yes | Yes | Required | Required |

Legend:
AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical/Mission Essential
PM = Program/Project Manager

* Although not required by DoD, the Component may require an Acquisition IA Strategy.
** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system

Source: Defense Acquisition Guidebook, Table 7.5.5.1. " IA Compliance by Acquisition Program Type"

# Acquisition IA Strategy Contents

1. **Program Category and Life Cycle Status:**
   - Acquisition Category (ACAT)
   - Acquisition Life cycle phase
   - Next milestone decision
   - Program schedule graphic
   - “Mission Critical” or “Mission Essential”

2. **Mission Assurance Category (MAC) and Confidentiality Level:**
   - As determined by information owner
   - Required for Baseline IA Controls

# Acquisition IA Strategy Contents

## 3. System Description:

- High-level overview
- Graphic (block diagram) of major elements/subsystems
- High level description of IA approach that will secure the system

## 4. Threat Assessment:

- Describe method/source
- DIA "Information Operations Capstone Threat Assessment“ for MAIS programs

## 5. Risk Assessment:

- Describe existing or planned regimen of assessments

# Acquisition IA Strategy Contents

## 6. Information Assurance Requirements:

- Describe sources of IA requirements (ORD, ICD, etc)
- Describe method for ensuring requirements are addressed early in the acquisition process, including DoDI 8500.2 controls
- Describe how requirements costs are included in budget

## 7. Acquisition Strategy:

- Summary of how IA is addressed in the program's overall acquisition strategy
- Describe how the RFP:
  - Includes IA requirements in performance or technical specification
  - Requires personnel trained in IA
- Address COTS IA or IA-Enabled products and approach towards NSTISSP 11 compliance

# Acquisition IA Strategy Contents

## 8. Certification and Accreditation:

- Method (i.e. NISCAP, DITSCAP)
- Identify DAA/PAA, CA, User Rep
- C&A boundaries
- Provide rough C&A timeline graphic

## 9. IA Testing:

- Describe how IA testing is integrated in TEMP

## 10. IA Shortfalls:

- Identify any known significant shortfalls
- Proposed approach to correct or mitigate
- Add classified annex, if required

# Acquisition IA Strategy Contents

## 11. Policy/Directives:

- Identify primary IA policy guidance employed by the program

## 12. Relevant Associated Program Documents:

- Identify specific version of applicable ORD/ICD/CDD/CPD
- Identify specific version of applicable ISP

## 13. IA Point of Contact:

- Preferably, the IA Manager for program

# Acquisition IA Strategy Approval and Review Process

***Required for every Milestone Decision, and Full Rate Production Decision (or equivalent):***

- **Early coordination reviews with DoD and Agency CIO IA Staff.**
- **Agency CIO Approval.**
- **Formal DoD CIO Review.**
- **CCA Certification Package Input (if appropriate).**

# Acquisition IA Strategy Informing the Acquisition

The value of an acquisition IA strategy is in its impact on program decision making and planning. There should be **recognizable synchronization** between the IA strategy and other key acquisition documents:

- **Capability/Requirements Documents (ORD, ICD,CDD, etc.)** should address
  - Specified IA requirements, including IA related KPPs
- **Acquisition Strategy** – should address
  - IA Technical considerations (e.g. COTS/NSTISSP 11)
  - IA Schedule considerations (e.g. C&A timeline and milestones)
  - IA Cost considerations (e.g. operations and maintenance)
  - IA Funding considerations (for full life cycle)
  - IA Staffing and Support considerations (e.g. organic, matrixed or contracted)
- **Test & Evaluation Master Plan (TEMP)** should address:
  - C&A roles/responsibilities (e.g. DAA, CA, OTA)
  - Integration of IA testing in DT and OT
  - Key events (e.g. IATO, ATO, IATT)

# Resources

- Your Agency CIO IA staff
- The IA Support Environment (IASE) Website (http://iase.disa.mil)
  - DoD IA Tools & Resources
  - IA Document Library
  - “Ask the Experts”
  - Policy and Guidance
  - Solutions Database
  - IA Training

# Resources (cont.)

## IA in Acquisition Website

DAU Acquisition Community Connection
IT Community of Practice (CoP)

**Location:**

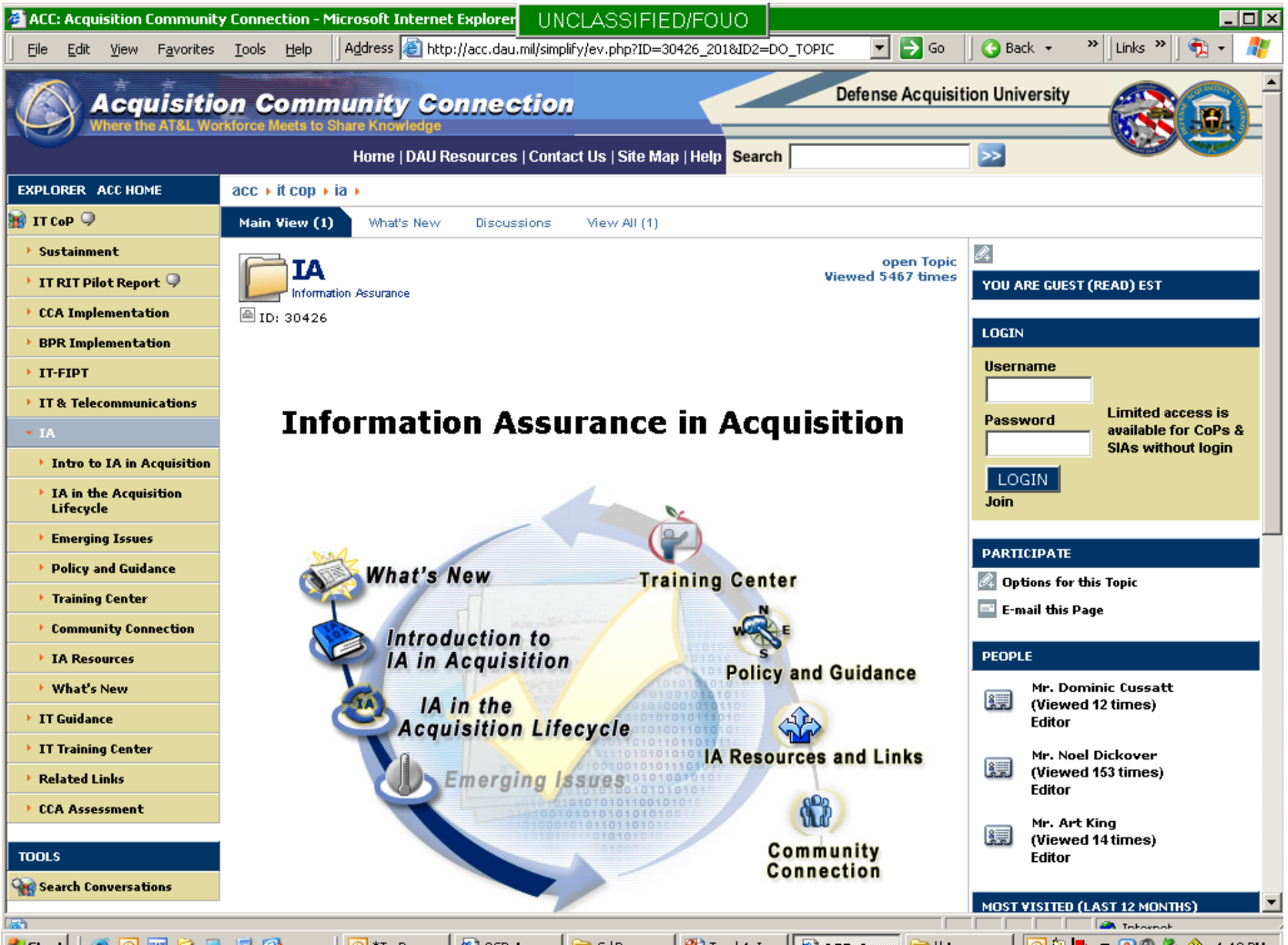
- http://acc.dau.mil
- Click on “IT CoP” Link

**Top Level Links for “Information Assurance (IA) in Acquisition”:**

1) Introduction to IA in Acquisition
2) IA in the Acquisition Lifecycle (The IA Roadmap)
3) Emerging Issues (Coming Soon)
4) Policy & Guidance Page
5) Training Center
6) Community Connection
7) IA Resource Links
8) What’s New

# Resources (cont.)

## IA in Acquisition Website



# Resources (cont.)

## DAU Learning Module "IA for PMs"

Located at the Defense Acquisition University's (DAU) Continuous Learning Center:

http://clc.dau.mil/kc/no_login/portal.asp

Course Name: "Information Assurance"

Description: Focuses on describing the importance of Information Assurance, the Program Manager's responsibilities, and steps for integrating IA into an acquisition program.

# Resources (cont.)

## DAU Learning Module “IA for PMs”

Defense Acquisition University's Continuous Learning Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://clc.dau.mil/kc/no_login/portal.asp
Go
Back
Links ANET A-Net Login Customize Links DAB Calendar Dictionary
Continuous Learning Center
Defense Acquisition University
Defense Acquisition University
Info | Map | Glossary | Search | Help
Select a function
Go
Login
Register
Conference Center
Learning Center
Library
Welcome to the CLC!
The Mission of the CLC is to provide a single portal for easy access to a multitude of continuous learning opportunities, performance support and information. This will help you, as a member of the Acquisition Community, fulfill the requirement of 80 continuous learning points every two years. Check back often. We are constantly changing to meet your needs. Need Assistance? Contact the DAU CLC team at TeamCLC or 1-866-568-6924 (toll free) or 703-805-3459 (commercial).
Announcements
New Deskbook Site
**International Armaments...
Communities of Practice Web...
more >>
FAQs
What is Systems Engineering?
How do I update my profile?
I click on a link but nothing...
more >>
Surveys
No Surveys available!
Learning Center
Personal CLC
Conference Center
Training Center
Library
Administration
Learning Center | Conference Center | Library
Use of this site signifies your agreement to the CLC Security & Privacy Policy.
THE ETHICS TRAINING MODULE IS NO LONGER AVAILABLE USING THE CLC. AS
Course Information & Enrollment
Internet

# Resources (cont.)

## DIAP Acquisition Team

***Role:*** **Advance the integration of IA in Acquisition Programs**

- Develop acquisition related IA policy and guidance
- Conduct outreach to acquisition programs
- Participate in IIPTs, OIPTs and select WIPTs
- Conduct DoD CIO reviews of IA Strategies (per CCA)
- Coordinate on MAIS/MDAP acquisition documents, including:
  - Test & Evaluation Master Plans (TEMP)
  - Systems Engineering Plans (SEP)
  - Acquisition Strategies
  - Acquisition Program Baselines (APB)
  - Acquisition Decision Memorandums (ADM)
- Review program IA implementation progress
- Develop acquisition IA training
- Act as focal point for acquisition related IA matters

# DIAP Acquisition Team
## *Points of Contact*


**Mr. Tom Anderson**
OASD(NII)/DIAP- Chief, Technologies and Capabilities
(703) 602-9969
Thomas.anderson@osd.mil

**Mr. Art King (IBM)**
(703) 604-1480 ext. 104
arthur.king.ctr@osd.mil

**Mr. Dominic Cussatt (IBM)**
(703) 604-1480 ext. 119
Dominic.cussatt.ctr@osd.mil

# Questions?